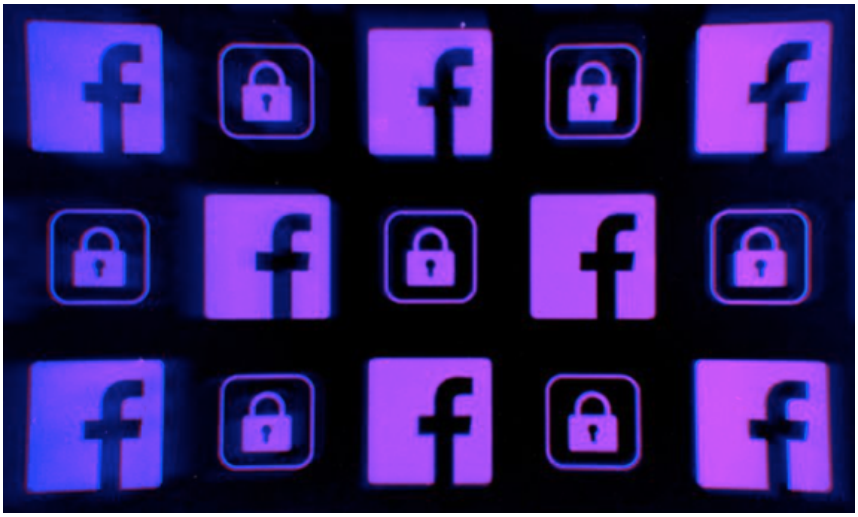
Volume #4 - Issue #180
October 5th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Latest Facebook Hack: How to Find Out If You're Affected & What To Do If You Are



Hackers may have gained access to nearly 50 million accounts by exploiting flaws in the social network's code, Facebook said Friday. It's the largest breach in the company's history. Facebook says it has notified law

enforcement officials and patched the code vulnerability that hackers exploited.

A lot of questions remain. We don't know for sure whether the impacted accounts were misused. It's also unclear exactly what information hackers may have accessed, though Facebook said passwords and payment information were not compromised. "So far, our initial investigation has not shown that these tokens were used to access any private messages or posts or to post anything to these accounts," CEO Mark Zuckerberg told reporters Friday. "But this, of course, may change as we learn more."

The attackers were able to use accounts as if they were their own by stealing "access tokens." Tokens keep users logged into their Facebook accounts over long periods of time without having to re-enter a password. Facebook said Friday that it reset all 50 million tokens, as well as tokens for an additional 40 million people as a "precautionary step." And there may be more to come. Facebook said an investigation into the breach has only just begun. "If we find more affected accounts, we will immediately reset their access tokens," the company said in a blog post.

Users that were logged out of their accounts can log back in using their usual passwords. They will then see a banner on top of their news feed that reads: "An important security update." It offers a link that gives you some details about the breach. Even if you're not one of the 90 million, Facebook suggested you log out of you account, as a "precautionary" step. That will reset your access tokens. You can do so from a desktop computer by clicking the arrow in the top right menu bar of your screen, selecting "Settings," and then navigating to the "Security and Login" tab. On Facebook's iPhone mobile app, tap the bottom right corner of the screen, scroll down, and tap "log out."

Facebook says access tokens, not passwords, were stolen. But Bruce Schneier, a top cybersecurity expert and fellow at the Harvard Kennedy School, said it's wise to take this step anyway. You can start this process from the "Security and Login" tab on your "Settings" page. Schneier also recommends turning on two-factor authentication. When it's activated, users are required to input a code at the time of login. You can choose whether you want to receive the code via text message or through a separate authentication app. To turn on two-factor authentication, use the "Security and Login" page.

After you reset your password, Facebook prompts you to review which devices had access to your account, just hit "Log out of other devices". Experts said to check where you're logged in on a regular basis. You can access this info on Facebook's "Security and Login" page. Facebook said it automatically unlinked potentially affected accounts from Instagram and Oculus, both of which are owned by Facebook. It did not do so with WhatsApp, which the company said was not impacted.
Facebook's vice president of product management, Guy Rosen, told reporters Friday that it wasn't clear if hackers were able to gain access to third-party apps that use Facebook login, but couldn't rule it out.
A wide range of sites use that feature, including payment apps like Venmo. "It's important to say: The attackers could use the account as if they are the account holder," Rosen said.

Experts say it's a good idea to reset all your passwords for apps that were linked to Facebook login anyway. Kevin Mitnick, a former hacker who founded cybersecurity consulting firm Mitnick Security, said he recommends using long, complex passwords and storing them with a password manager such as 1Password or KeePass. He says your primary password should be long. "Over 25 characters," he said.

You can check which external apps you have authorized on Facebook's "Settings" page under the "Apps and Websites" tab.
Schneier, the cybersecurity expert, said if you can stand to remember a few more logins and passwords, it's a good idea to unlink Facebook from all of them.

It's wise to trash anything on your Facebook profile you don't want out in the open, experts say. Go through old messages, photos, and posts — and start deleting. Schneier, the Harvard Kennedy School lecturer, said if you are online, it's best to always be cautious about what you share. You are completely at their mercy, and you have to hope for the best, and that's true of any tech firm you share information with.

Remember, as with any free service, you are not the customer, you are the product!

Thank you for subscribing to our email!